杭州电子科技大学

网络安全理论与技术实验

实 验 报 告

学　　院	网络空间安全学院
专　　业	网络工程
班　　级	18272412
学　　号	18041618
学生姓名	廖越强
教师姓名	高梦州
完成日期	2020.12.4
成　　绩	

实验一　钓鱼网站实验

一、　实验目的

(1)验证伪造的 DHCP 服务器为终端提供网络信息配置服务的过程。

(2)验证错误的本地域名服务器地址造成的后果。

(3)验证利用网络实施钓鱼网站的过程。

二、　实验原理

终端通过广播 DHCP 发现消息发现 DHCP 服务器,当 DHCP 服务器与终端不在同一个网络(同一个广播域)时,由路由器完成中继过程。DHCP 服务器通过向终端发送 DHCP 提供消息表明可以为终端提供网络信息配置服务,终端选择发送第一个到达终端的 DHCP 提供消息的 DHCP 服务器为其提供网络信息配置服务。

如图 2.38 所示,在终端连接的网络中接入伪造的 DHCP 服务器后,终端广播的 DHCP 发现消息到达伪造的 DHCP 服务器,伪造的 DHCP 服务器在网络中广播 DHCP 提供消息,由于伪造的 DHCP 服务器与终端位于同一网络,伪造的 DHCP 服务器发送的 DHCP 提供消息可能先于 DHCP 服务器发送的 DHCP 提供消息到达终端，导致终端选择伪造的 DHCP 服务器为其提供网络信息配置服务，并将伪造的 DNS 服务器的 IP 地址 192.1.3.1 作为本地域名服务器地址。

三、　实验环境/实验拓扑图

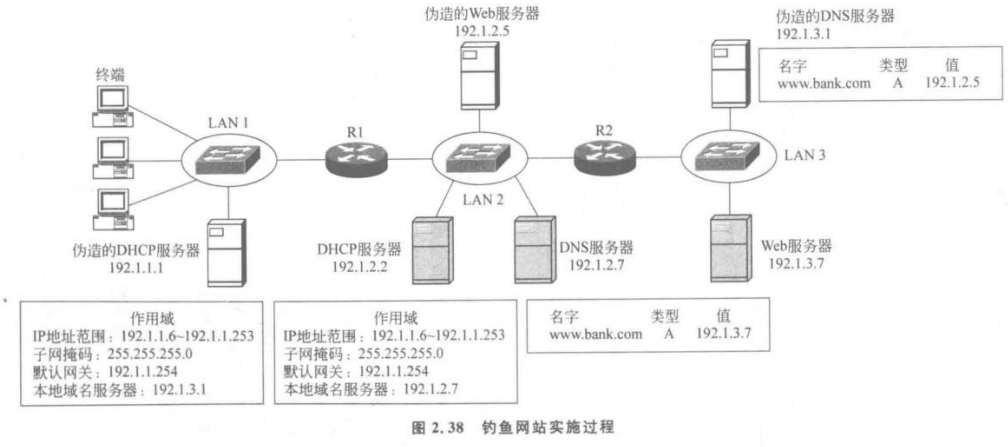
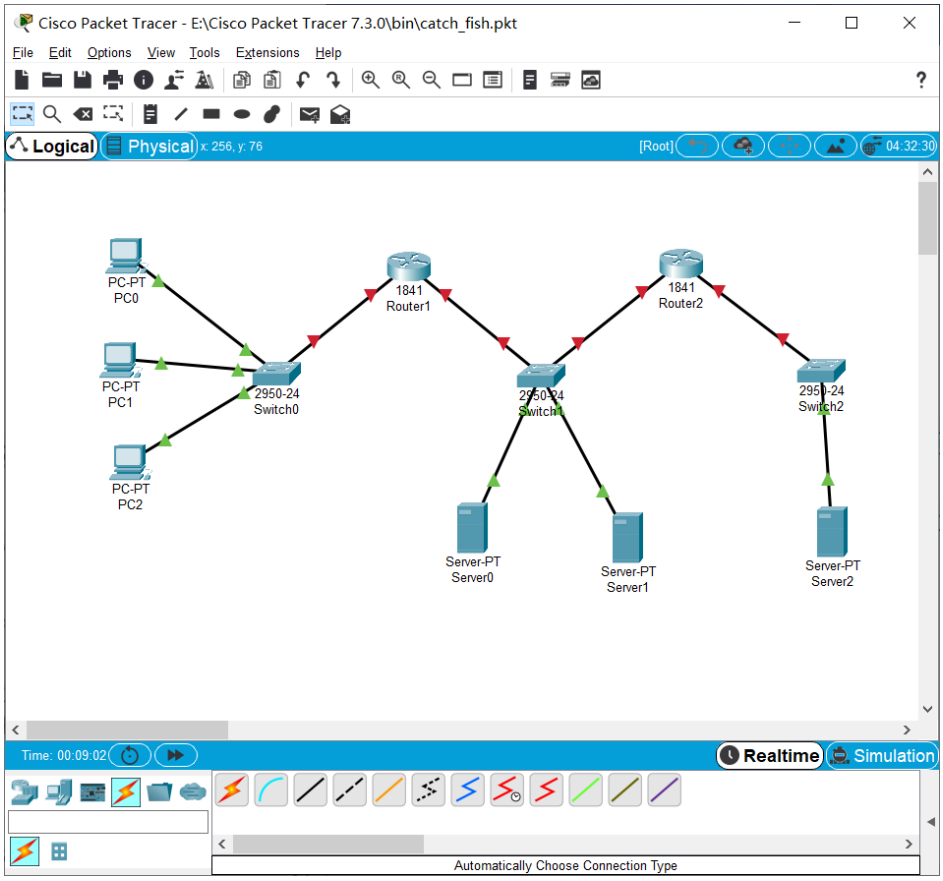


图 2.38　钓鱼网站实施过程

四、 主要操作步骤及实验结果记录

1. 完成拓扑图连接



2. 配置路由器接口 IP 地址和掩码，完成路由器 RIP 配置

router1 路由表

```
C    192.1.1.0/24 is directly connected, FastEthernet0/0
C    192.1.2.0/24 is directly connected, FastEthernet0/1
R    192.1.3.0/24 [120/1] via 192.1.2.253, 00:00:10,
FastEthernet0/1

Router#
```

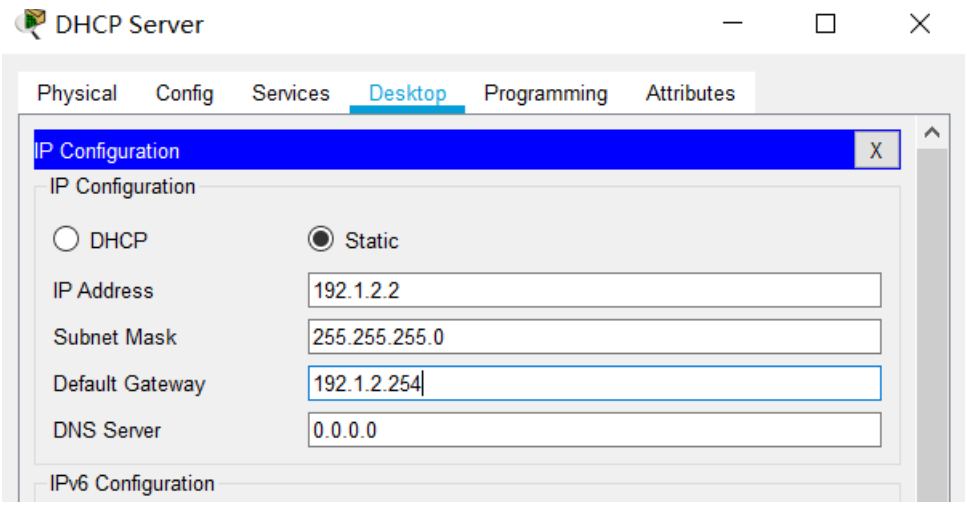
router2 路由表

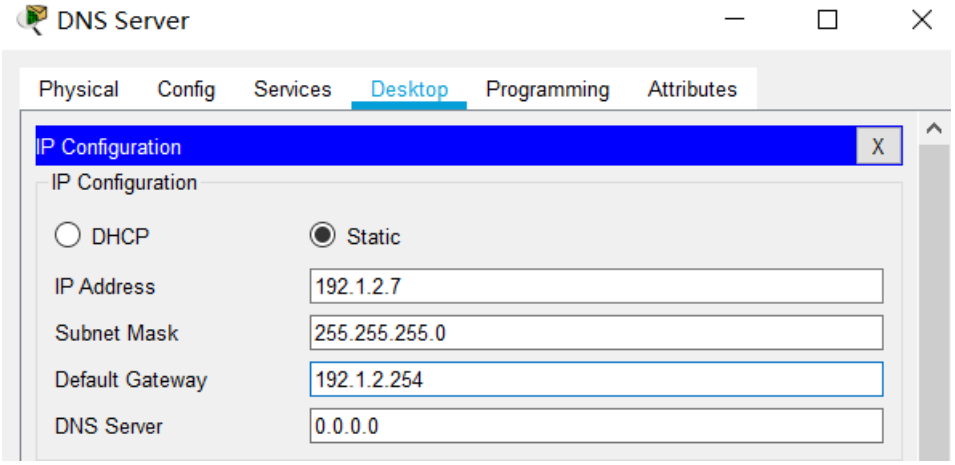
```
R    192.1.1.0/24 [120/1] via 192.1.2.254, 00:00:26, FastEthernet0/0
C    192.1.2.0/24 is directly connected, FastEthernet0/0
C    192.1.3.0/24 is directly connected, FastEthernet0/1

Router#
```

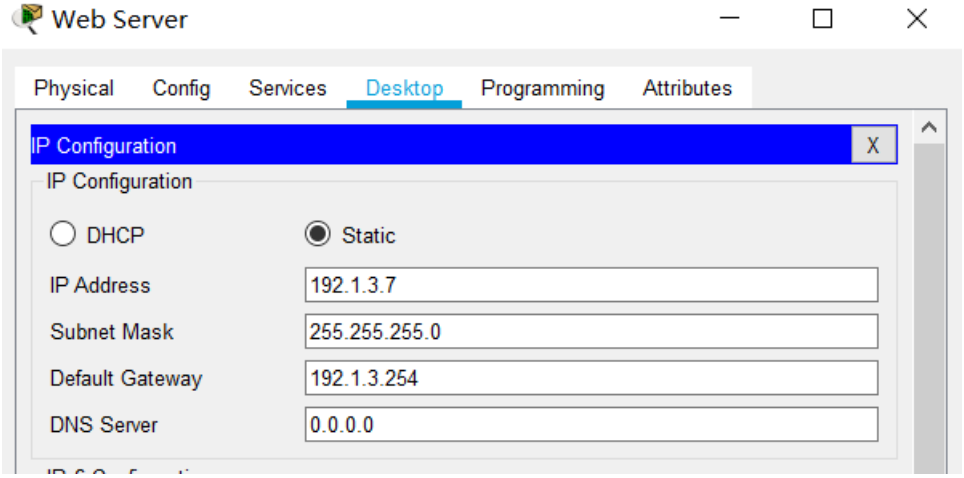
3. 完成 router1 接口 fastethernet0/0 的中继地址配置

```
Router(config)#interface fastEthernet 0/0
```

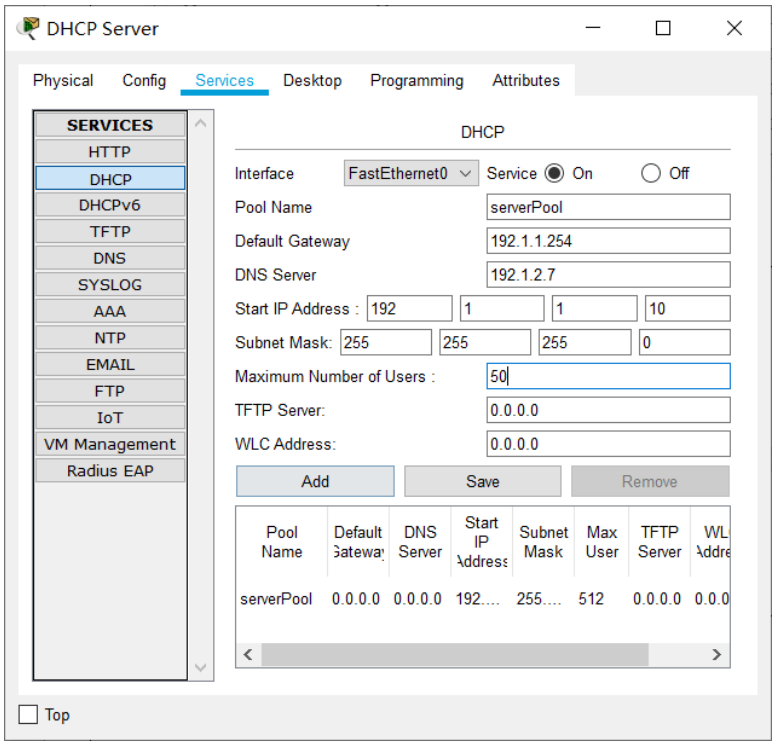
4. 完成 3 台服务器的 IP 地址、子网掩码和默认网关的配置



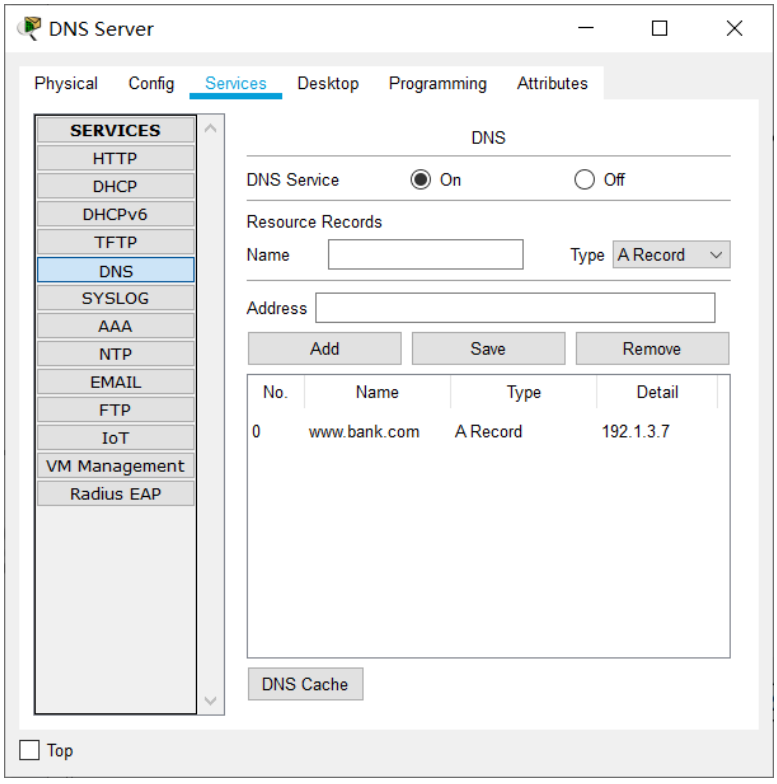




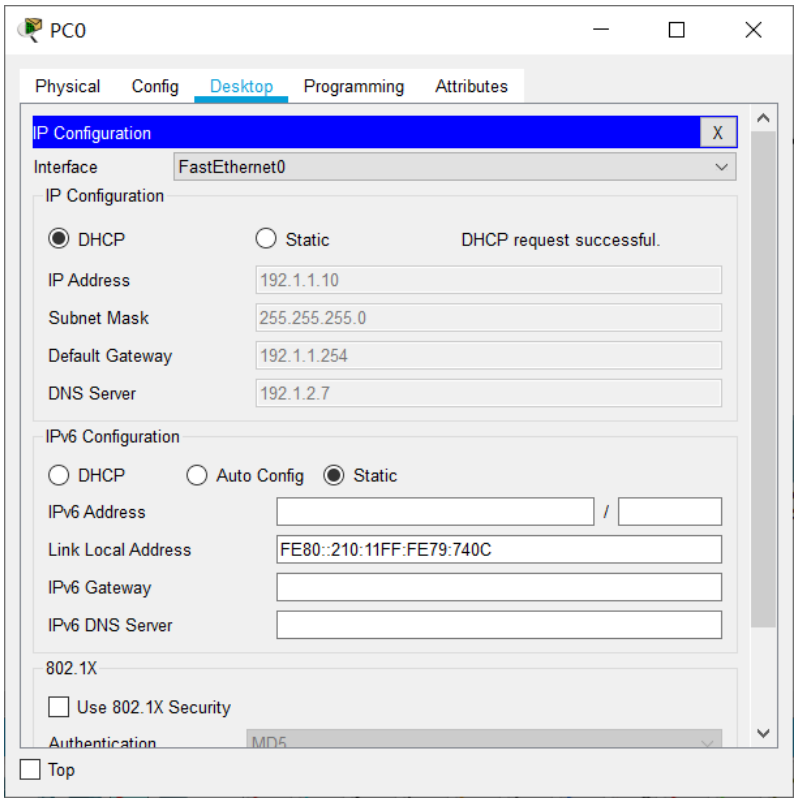
5. 开启 DHCP 服务器的“DHCP”功能，并配置



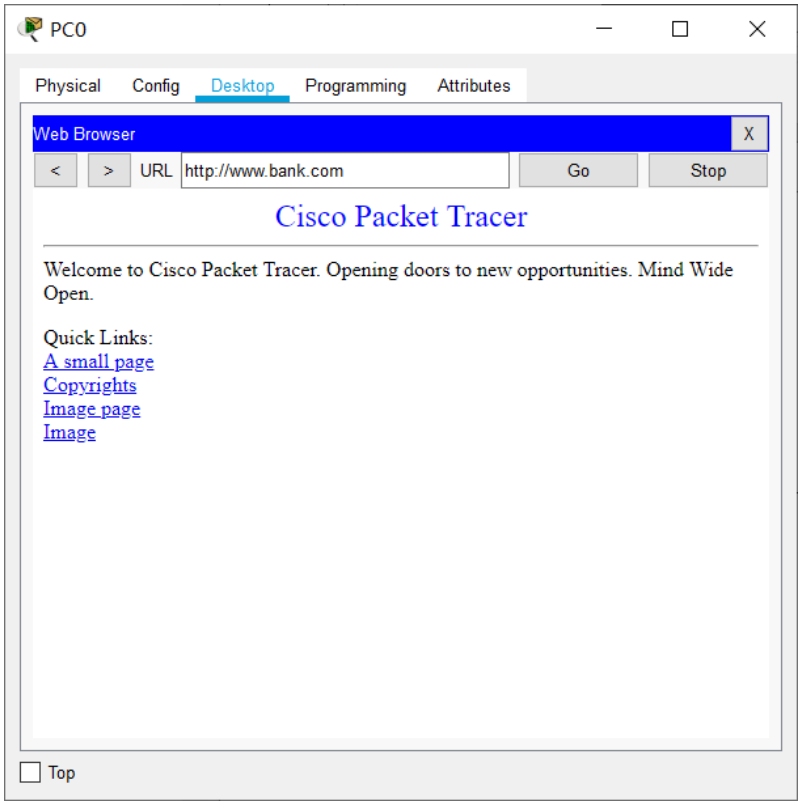
6. 配置 DNS 服务器，并添加记录



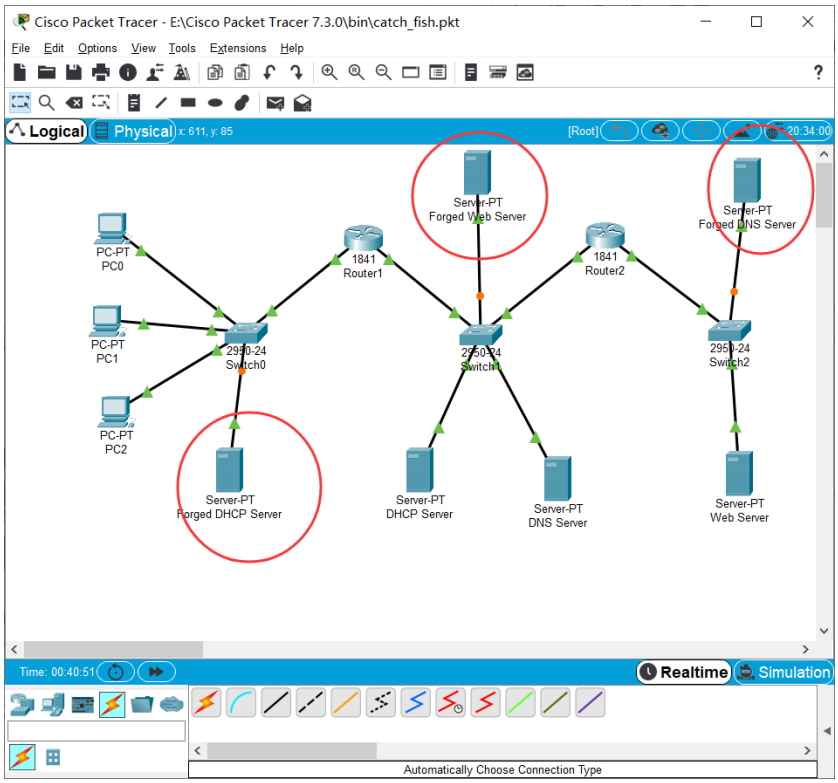
7. 配置 pc0，使用 DHCP 模式



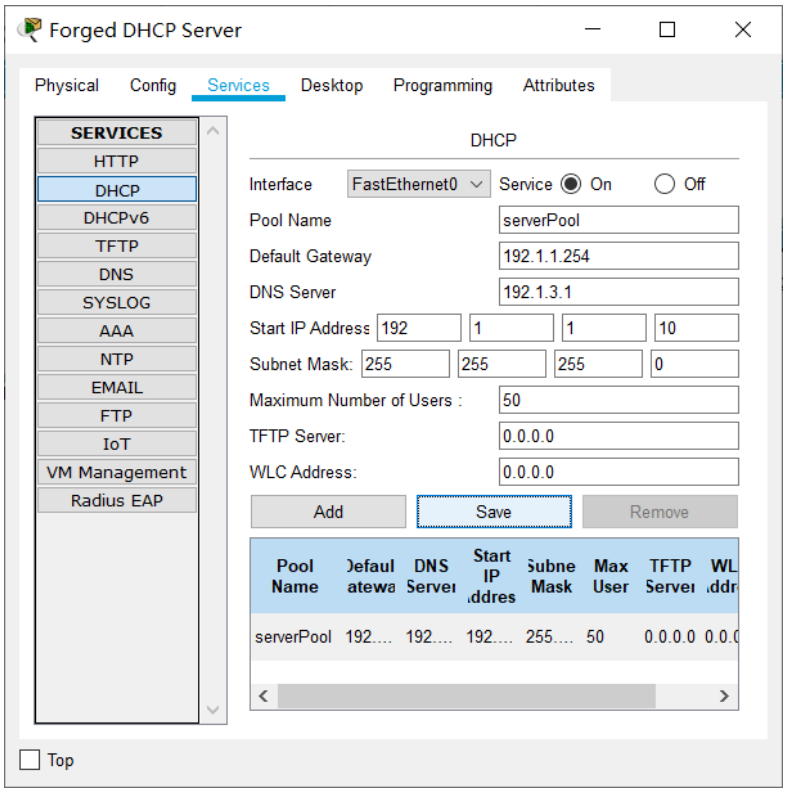
8. 使用 pc0 通过域名访问 web server



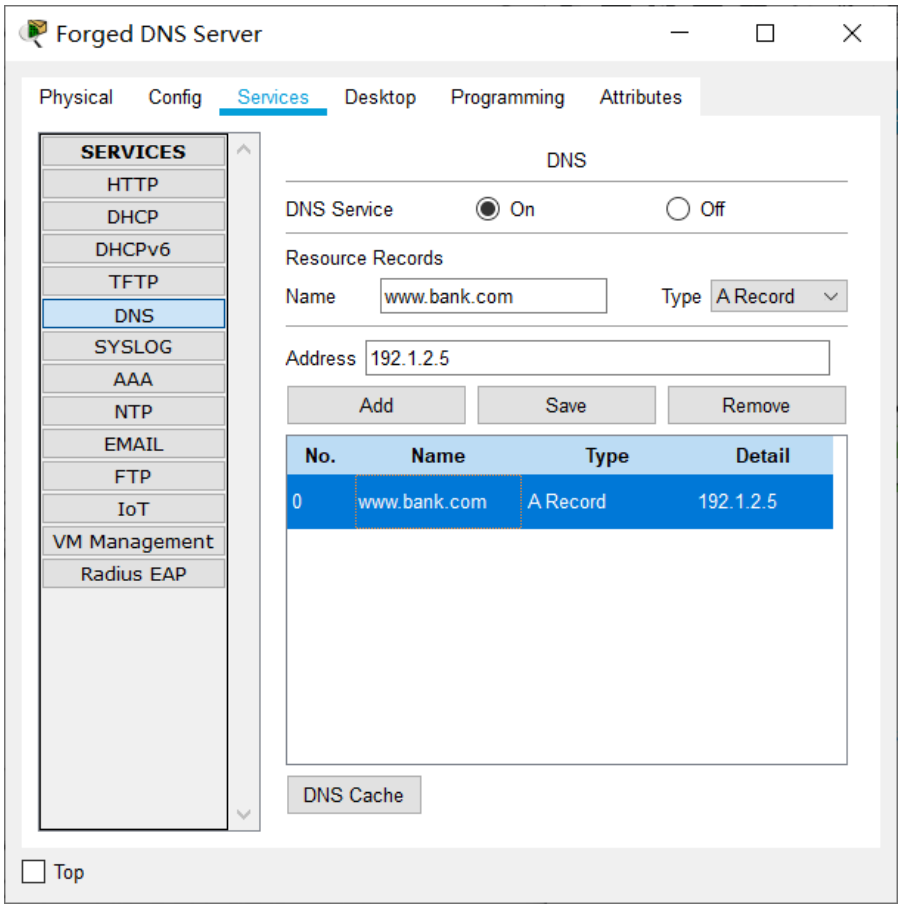
9. 接入 3 台伪造的服务器，并完成其 IP、子网掩码、默认网关的配置



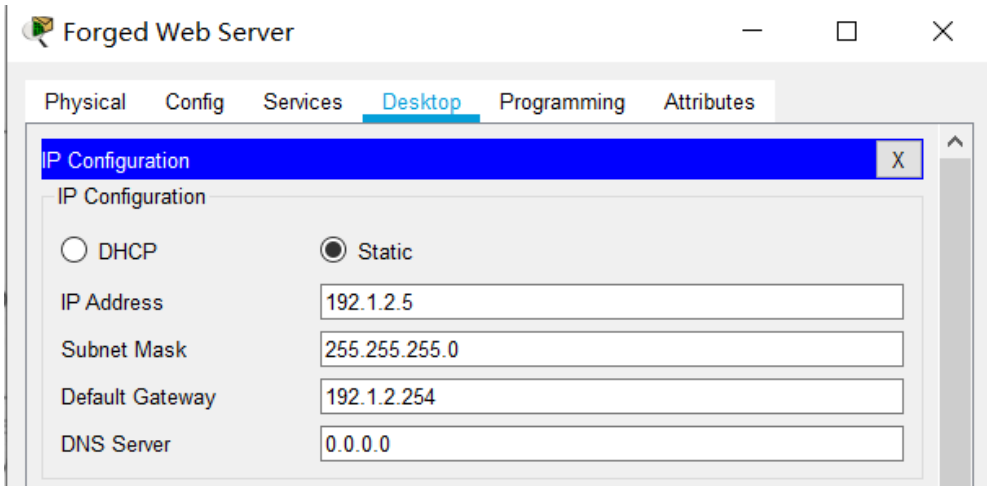
伪造的 DHCP 配置



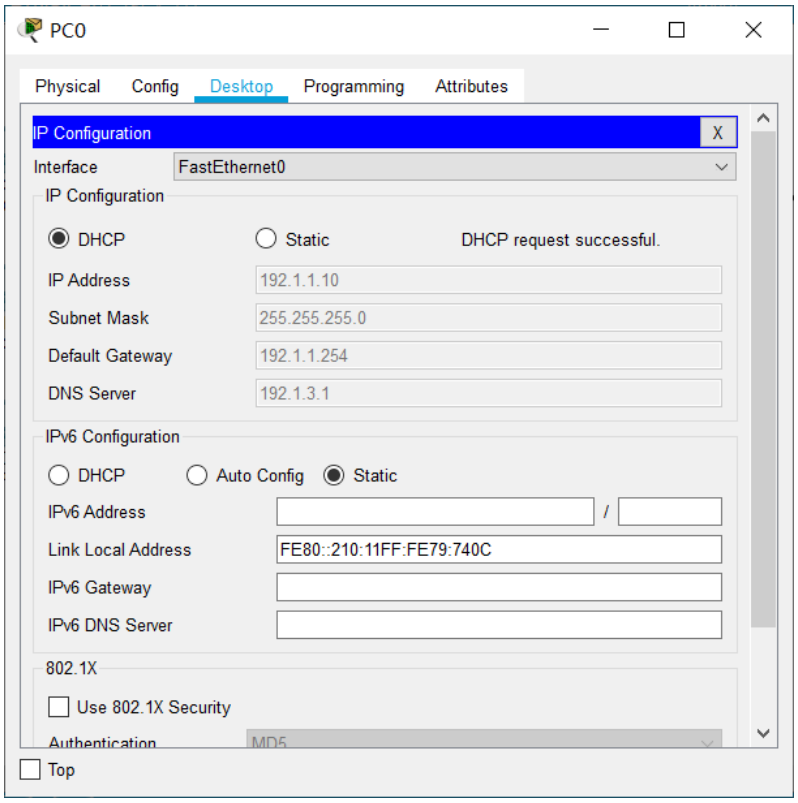
伪造的 DNS 服务器配置



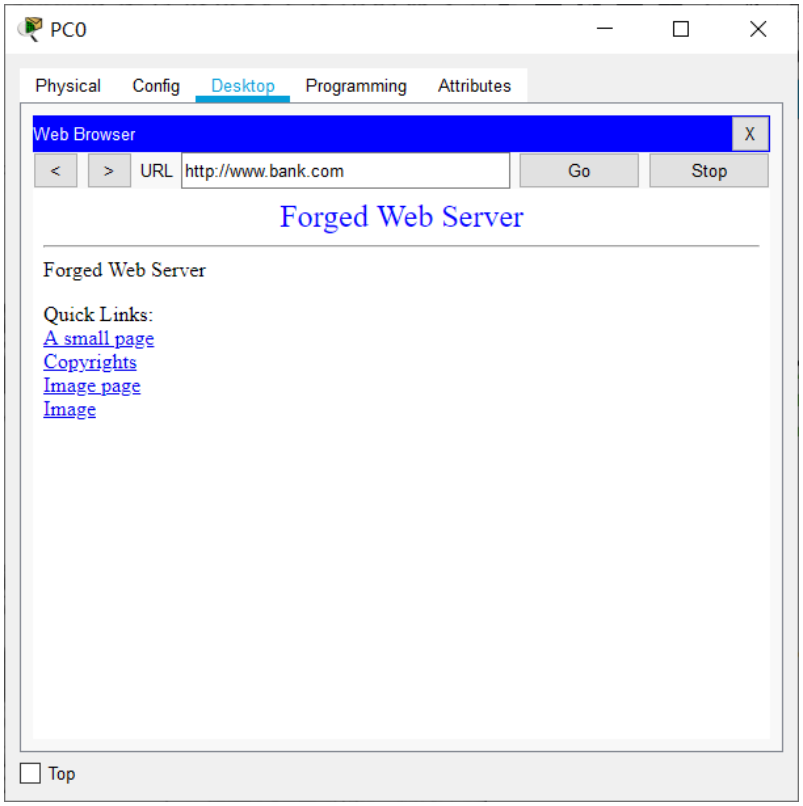
伪造的 Web 服务器配置



使用 pc0 再次使用 DHCP 获取地址，可见 DNS Server 变成了 192.1.3.1，表明从伪造的 DHCP 服务器获取网络信息



10. 使用 pc0 访问伪造的 web Server



五、 实验分析总结及心得

1) **命令列表**

ip helper-address address 一是配置 DHCP 服务器的 IP 地址,二是启动接口的 DHCP 中继功能。参数 address 给出 DHCP 服务器的 IP 地址

2) **总结心得**

配置 DHCP 配完后记得点 save，直接退出的话，配置是不会生效的。

通过这次实验，我对 DHCP 这方面的安全知识有了新的认识，对黑客利用 DHCP 服务器接入网络的攻击流程有了一个的清晰的认识。也对通过 DHCP 获取网络信息这个概念有了更深入的理解，意识到了需要对 DHCP 进行一些防护，提高网络防护安全，提高了自己的安全意识。

实验一　防 DHCP 欺骗攻击实现

六、　实验目的

(1)验证 DHCP 服务器配置过程。

(2)验证 DNS 服务器配置过程。

(3)验证终端用完全合格的域名访问 Web 服务器的过程。

(4)验证 DHCP 欺骗攻击过程。

(5)验证钓鱼网站实施过程。

(6)验证交换机防 DHCP 欺骗攻击功能的配置过程。

七、　实验原理

终端通过 DHCP 自动获取的网络信息中包含本地域名服务器地址,对于如图 4.7 所示的网络应用系统,DHCP 服务器中给出的本地域名服务器地址是 192.1.2.7,地址为 192.1.2.7 的域名服务器中与完全合格的域名 www.bank.com 绑定的 Web 服务器地址是 192.1.3.7。因此,终端可以用完全合格的域名 www.bank.com 访问 Web 服务器。

一旦终端连接的网络中接入伪造的 DHCP 服务器,终端很可能从伪造的 DHCP 服务器获取网络信息,得到伪造的域名服务器的 IP 地址 192.1.3.1 ,伪造的域名服务器中将完全合格的域名 www.bank.com 与伪造的 Web 服务器的 IP 地址 192.1.2.5 绑定在一起,导致终端用完全合格的域名 www.bank.com 访问伪造的 Web 服务器。

如果交换机启动防 DHCP 欺骗攻击的功能,只有连接在信任端口的 DHCP 服务器才能为终端提供自动配置网络信息的服务。因此,对于如图 4.7 所示的实施 DHCP 欺骗攻击的网络应用系统,连接终端的以太网中,如果只将连接路由器 Rl 的交换机端口设置为信任端口,将其他交换机端口设置为非信任端口,则终端只能接收由路由器 Rl 转发的 DHCP 消息，使终端只能获取 DHCP 服务器提供的网络信息。

八、　实验环境/实验拓扑图

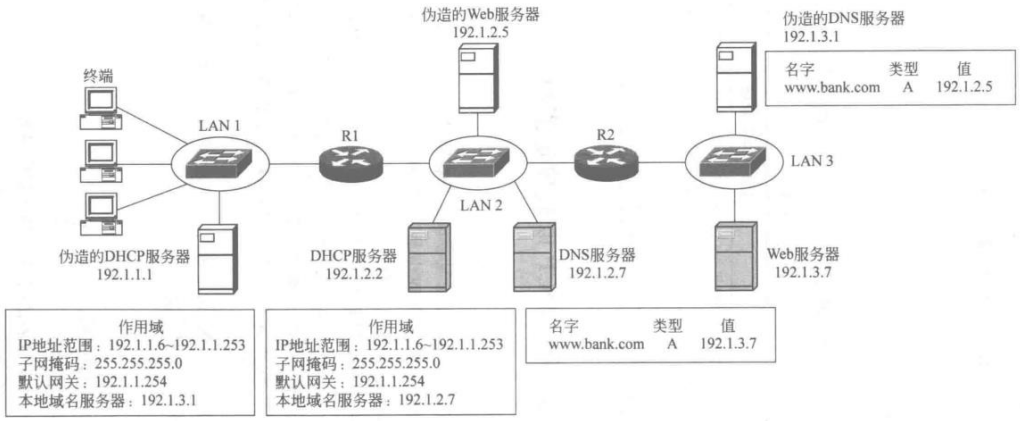
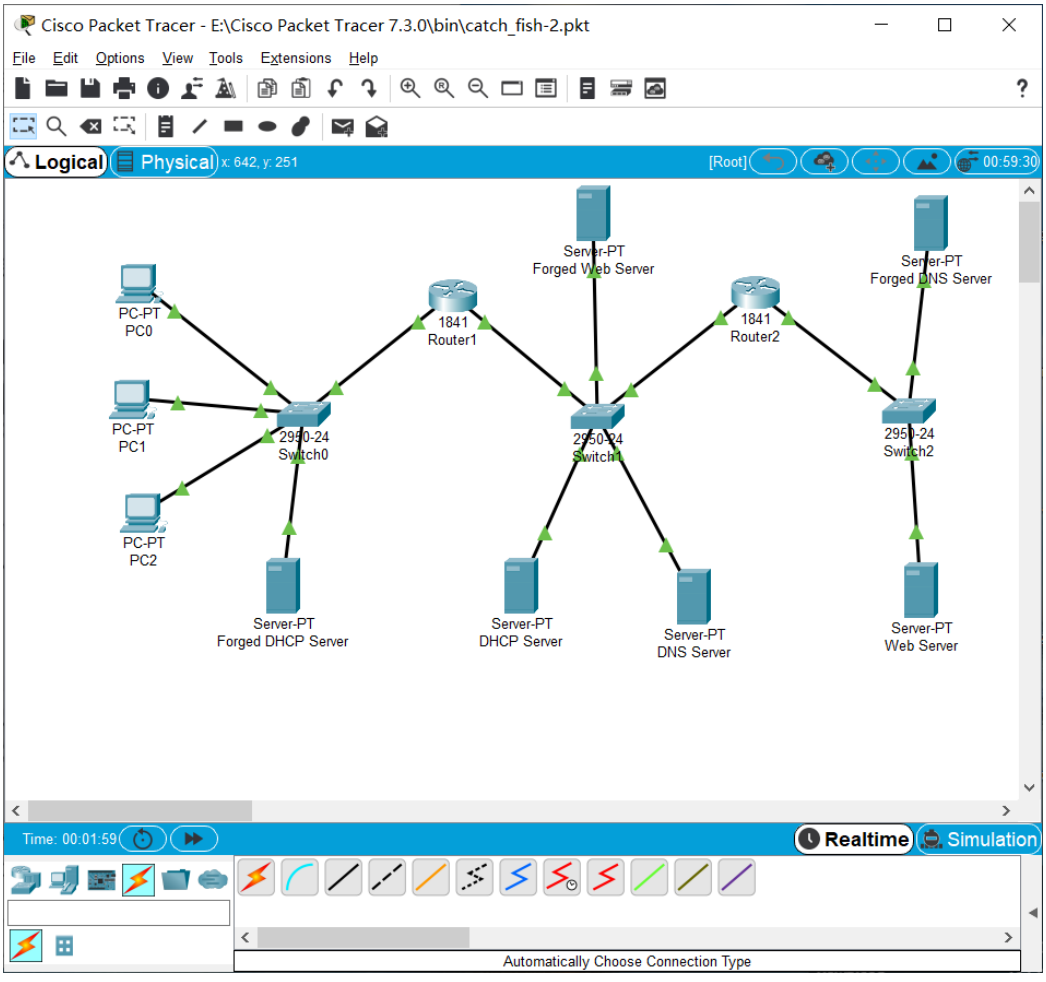


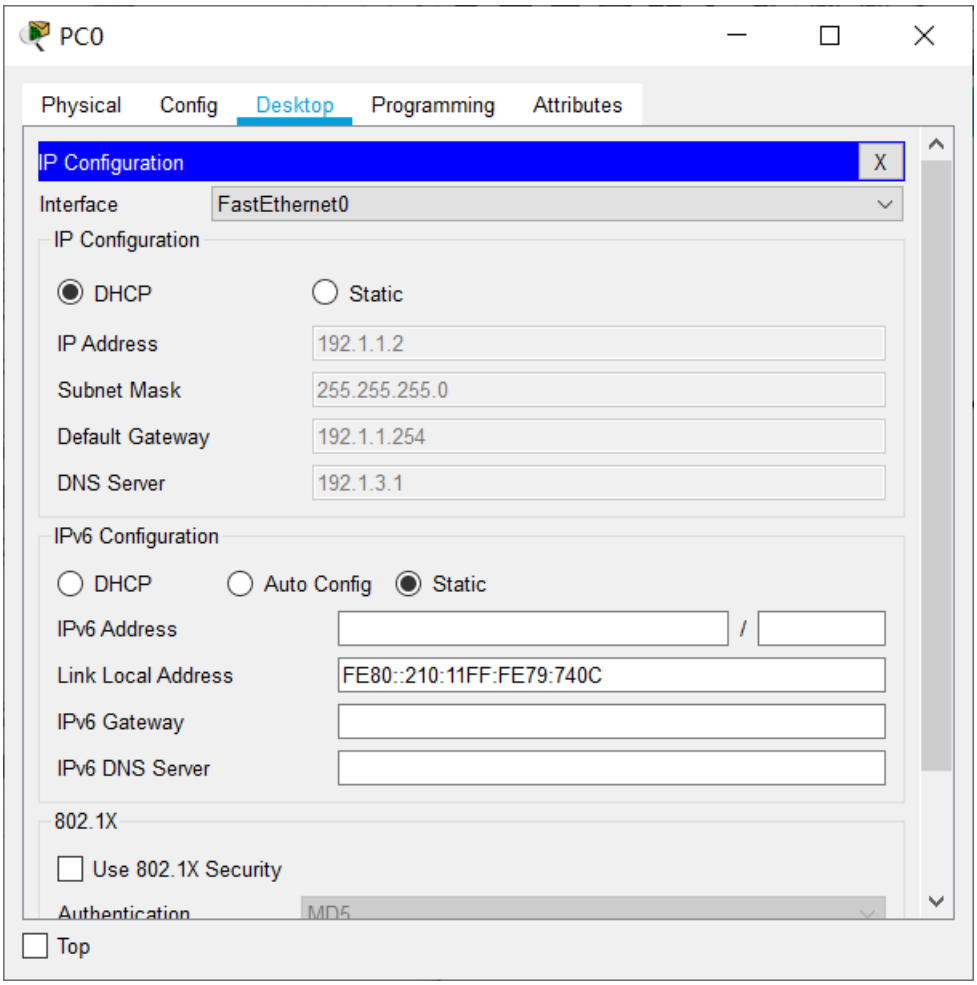
图 4.7 用于实施 DHCP 欺骗攻击的网络结构

九、 主要操作步骤及实验结果记录

1. 使用第 2.5 节的拓扑图



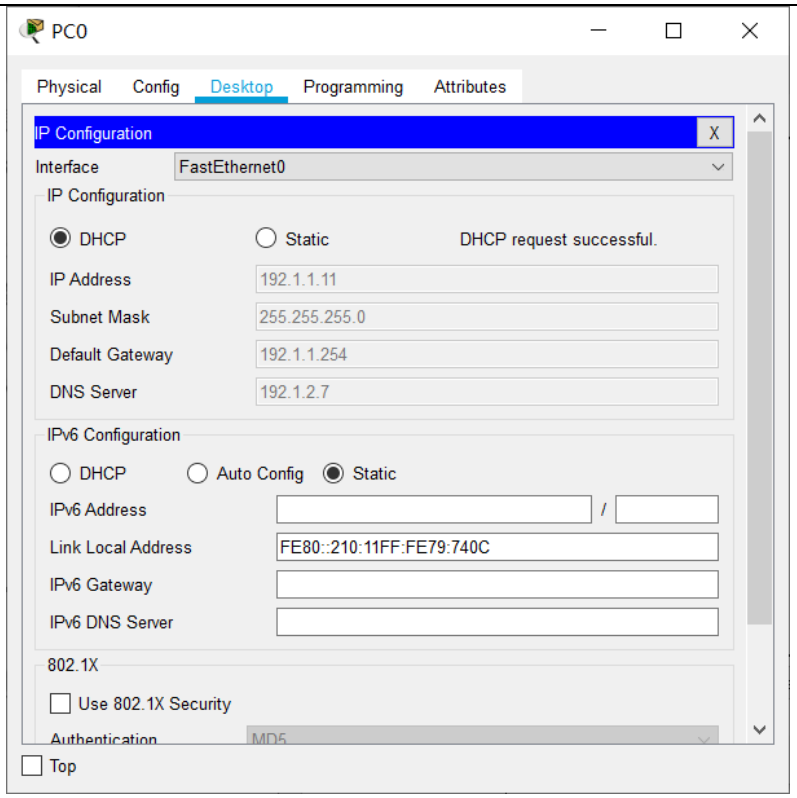
2. 启动交换机 switch0 防 DHCP 欺骗攻击的功能前，pc0 很可能从伪造的 DHCP 服务器获取网络信息，如图。

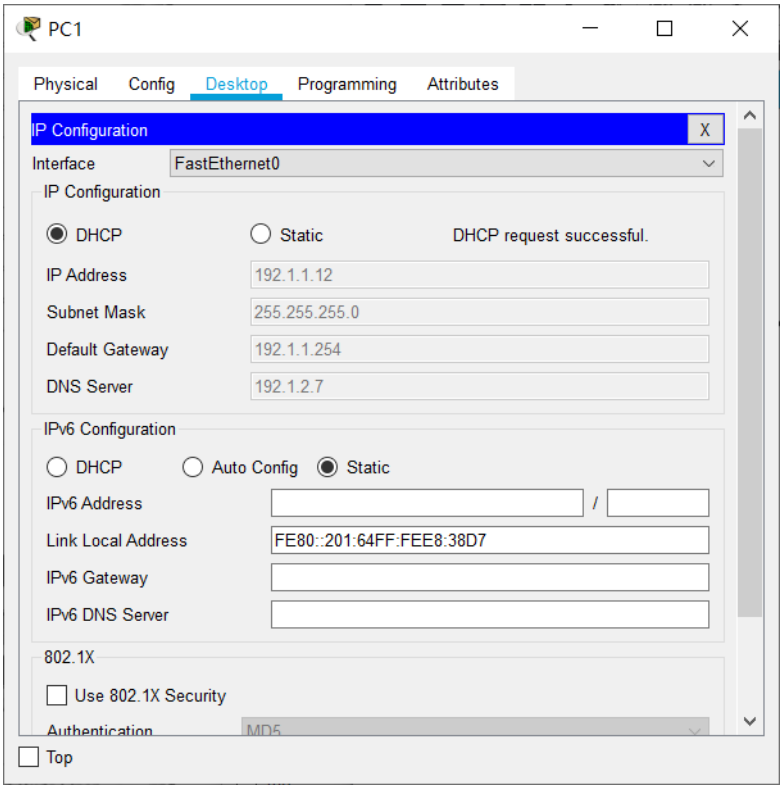


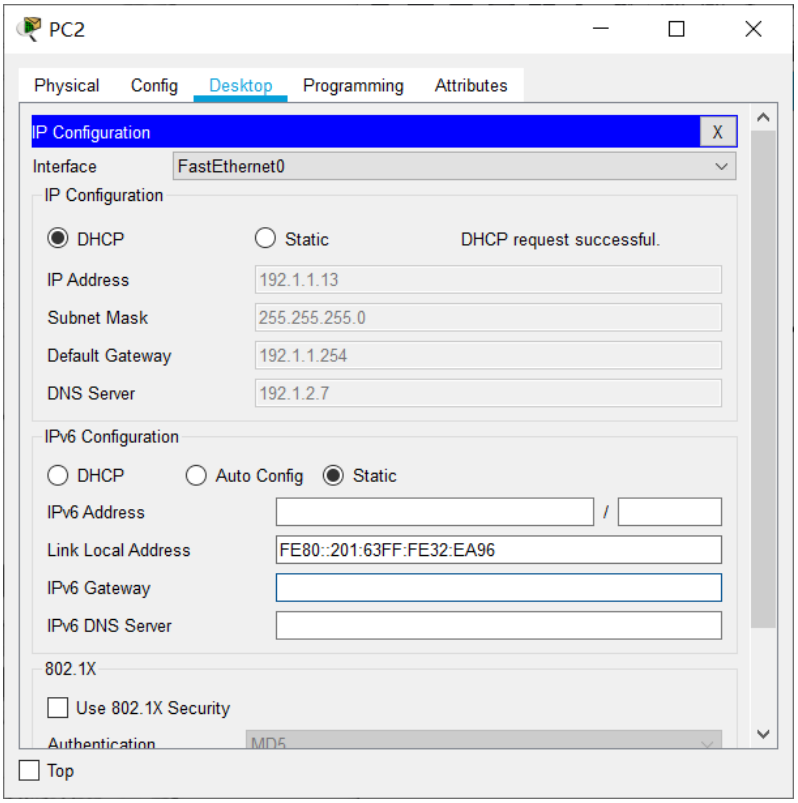
3. 在 switch0 CLI 下启动交换机防 DHCP 欺骗攻击的功能

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#inter
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/4
Switch(config-if)#ip dhcp snooping tru
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
Switch(config)#
```

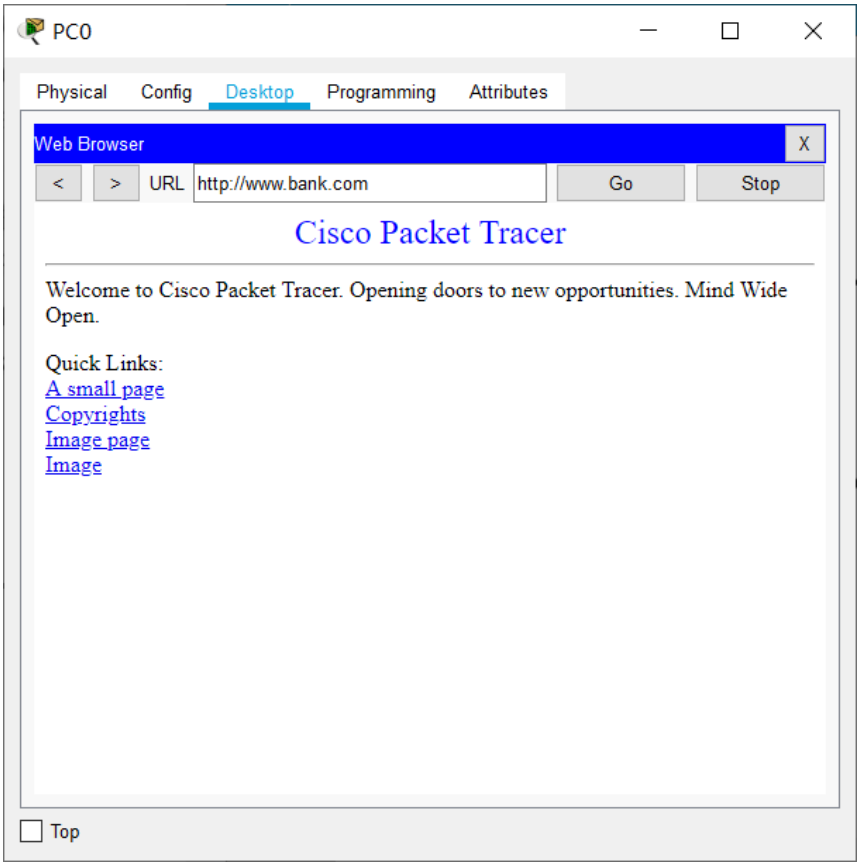
再使用 pc0、pc1、pc2 通过 DHCP 获取网络信息，可从正确的 DHCP 处得到网络信息，DHCP 地址为 192.1.2.7


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.1.1.11
Subnet Mask
255.255.255.0
Default Gateway
192.1.1.254
DNS Server
192.1.2.7
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::210:11FF:FE79:740C
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Top


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.1.1.12
Subnet Mask
255.255.255.0
Default Gateway
192.1.1.254
DNS Server
192.1.2.7
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:64FF:FEE8:38D7
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Top



使用 pc0 访问 www.bank.com 域名，访问到正确的 Web Server，如图



4. 显示 switch0 的 DHCP 侦听信息库，得到三者的绑定关系：pc 的 mac 地址、DHCP 分配给 pc 的 IP 地址和 Switch0 连接 pc 的交换机接口

```
Switch#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:10:11:79:74:0C   192.1.1.11       86400       dhcp-snooping  1     FastEthernet0/1
00:01:64:E8:38:D7   192.1.1.12       86400       dhcp-snooping  1     FastEthernet0/3
00:01:63:32:EA:96   192.1.1.13       86400       dhcp-snooping  1     FastEthernet0/2
Total number of bindings: 3
Switch#
```

十、 实验分析总结及心得

1. 命令列表

1. **ip dhcp snooping**

   启动 DHCP 侦听功能

2. **ip dhcp snooping vlan vlan-range**

   针对一个或一组 VLAN 启动 DHCP 侦听功能。参数 vlan-range 可以是单个 VLAN ID,或是多个用逗号分隔的 VLAN ID,或是一组连续的 VLAN ID

3. **ip dhcp snooping trust**

   将交换机端口设置为信任端口

4. **show ip dhcp snooping binding**

   显示 DHCP 侦听信息库中的内容,即 MAC 地址,IP 地址和交换机端口之间的绑定关系

2. 总结

通过这次实验，我对 DHCP 这方面的安全知识有了新的认识，学会了防御伪造的 DHCP 服务器接入网络的基本操作，对它们的攻击流程有了一个的深刻的认识。也对通过 DHCP 获取网络信息这个概念有了更深入的理解，明白了做好 DHCP 防御，提高网络防护的重要性，提高了自己的安全意识。